David M. Berger (SBN 277526)
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9713
Facsimile: (510) 350-9701
dmb@classlawgroup.com

Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
Kasey Youngentob (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100 (tel.)
siegel@stuevesiegel.com
moore@stuevesiegel.com
youngentob@stuevesiegel.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ABBY LINEBERRY, TERRY MICHAEL COOK and MIGUEL CORDERO, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

ADDSHOPPERS, INC., and PEET'S COFFEE, INC.,

Defendants.

Case No. 3:23-cv-01996-VC

PLAINTIFFS' MOTION FOR CLASS CERTIFICATION AND MOTION TO EXCLUDE EXPERT TESTIMONY AND MEMORANDUM IN SUPPORT

Judge: Hon. Vince Chhabria

Hearing: March 20, 2025

Time: 10:00 a.m.

Courtroom: 4

PLEASE TAKE NOTICE that on March 20, 2025 at 10:00 am, the undersigned will appear before the Honorable Vince Chhabria of the United States District Court for the Northern District of California at the San Francisco Courthouse, Courtroom 4, 17th Floor, 450 Golden Gate Avenue, San Francisco, California, 94102, and will move the Court, under Federal Rule of Civil Procedure 23, for an order certifying the following Propose Classes:

Under Fed. R. Civ. P. 23(b)(3)

Class	**Representatives**	**Defendant**
Nationwide CDAFA Class: All natural persons who visited Peet's website and for whom AddShoppers collected their detailed browsing activity.	Terry Michael Cook Miguel Cordero	Peet's Coffee, Inc.
California CIPA Subclass: All natural persons who, while in California, visited Peet's website for whom AddShoppers collected their detailed browsing activity.	Miguel Cordero	Peet's Coffee, Inc.
California CDAFA and CIPA Subclass: All natural persons who, while in California, visited Peet's or Dia's websites for whom AddShoppers collected their detailed browsing activity.	Abby Lineberry Miguel Cordero	AddShoppers, Inc.

Under Fed. R. Civ. P. 23(b)(2)

Class	**Representatives**	**Claims**
California Injunctive Relief Class: All natural persons who, while in California, visited a website for whom AddShoppers collected their detailed browsing activity.	Abby Lineberry Miguel Cordero	Against AddShoppers, Inc. in connection with their CDAFA and CIPA claims.

Plaintiffs seek the appointment of these Plaintiffs as class representatives. Plaintiffs also seek appointment of Norman Siegel, J. Austin Moore, and Kasey A. Youngentob from Stueve Siegel Hanson and David Berger from Gibbs Law Group as class counsel.

This motion is based on this notice, the memorandum of law, the declaration of Kasey A. Youngentob, the Plaintiffs' declarations, all exhibits to such documents, any papers filed in reply, and any argument as may be presented at the hearing.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

I. Introduction

This case is ideal for class certification. When visitors to Peet's Coffee, Inc.'s website viewed multiple webpages (one with a product) or added items to their carts, AddShoppers automatically collected their detailed browsing data. No exceptions, no variations. The tracking code works the same way for everyone, every time.

The system's uniformity stems from AddShoppers' streamlined approach: retailers simply copy and paste the company's JavaScript tracking code onto their websites, choose behavioral triggers, and the data collection starts. The code is designed to capture detailed records of consumers' product views, shopping cart contents, and other private browsing data—all without consent. AddShoppers then combines this surveillance data with millions of consumer records purchased from shadowy data brokers to track individuals across devices and websites, building comprehensive profiles that link personal information with detailed browsing histories.

This standardized tracking scheme presents textbook questions for classwide resolution: did AddShoppers violate the California Invasion of Privacy Act (CIPA) by intercepting communications without consent? Did Defendants access consumers' data without permission in violation of the California Computer Data Access and Fraud Act (CDAFA)? The answers apply uniformly to all class members because AddShoppers' system impacted everyone the same way.

To keep the case focused and manageable, Plaintiffs narrowly tailored their proposed classes to focus on tracking on specific retailers' websites whose privacy policies failed to disclose these tracking practices. With uniform statutory damages, clear liability questions, and AddShoppers' own database identifying class members, this case presents an ideal vehicle for class-wide resolution. The Court should therefore certify their proposed classes under Federal Rules of Civil Procedure 23(b)(2) and (b)(3).

II. Background

A. AddShoppers creates a marketing program to track anonymous shoppers across the internet.

[redacted] By early 2019, AddShoppers pivoted to a new marketing platform called SafeOpt.[3]

SafeOpt marked a significant departure from AddShoppers' original approach. [redacted], SafeOpt tracks anonymous shoppers across many retail websites, even when they use different devices.[4] In April 2018, AddShoppers published a blog post introducing its new product and describing the solution it provides:

Send 2x-5x more personalized triggered emails with incremental campaigns.

The Problem

Marketers are unable to send email reliably to customers that have not provided their email previously. This means more than 95% of your web visitors cannot receive a relevant email from you.

The Solution

Connecting the AddShoppers network of 150M+ shoppers through its Email Retargeting® Co-op, marketers are able to resolve identities and deliver 1:1 email regardless of customer email acquisition.

---

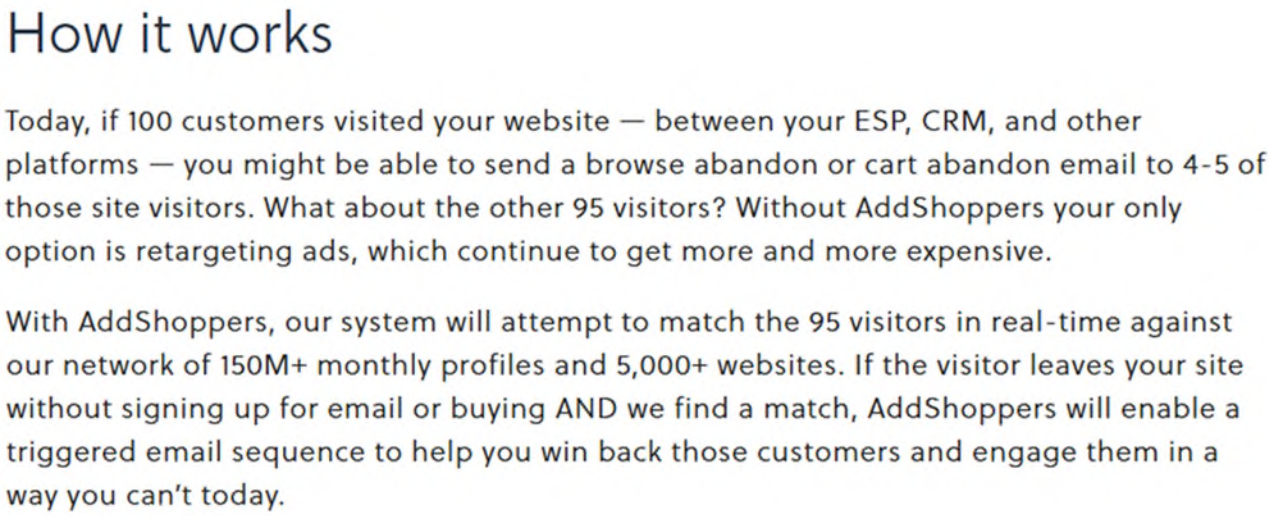
[1] West Dep. 29:13-25 (the West deposition transcript is attached to the Youngentob Declaration as Ex. 1); Ledford Dep. 25:19-26:2 (the Ledford deposition transcript is attached to the Youngentob Declaration as Ex. 2.

[2] Ex. 2, Ledford Dep. 29:16-30:15; 79:2-7.

[3] Ex. 1, West Dep. 17:19-20.

[4] King Dep. 71:16-18 (the King deposition transcript is attached to the Youngentob Declaration as Ex. 3); *id*. 146:23-147:7; Ex. 4.

In describing how the product works, AddShoppers represented that its system would "attempt to match the 95 visitors in real-time against [its] network of 150M+ monthly profiles and 5,000+ websites" [5]:



How it works

Today, if 100 customers visited your website — between your ESP, CRM, and other platforms — you might be able to send a browse abandon or cart abandon email to 4-5 of those site visitors. What about the other 95 visitors? Without AddShoppers your only option is retargeting ads, which continue to get more and more expensive.

With AddShoppers, our system will attempt to match the 95 visitors in real-time against our network of 150M+ monthly profiles and 5,000+ websites. If the visitor leaves your site without signing up for email or buying AND we find a match, AddShoppers will enable a triggered email sequence to help you win back those customers and engage them in a way you can't today.

In client-facing materials, AddShoppers describes using SafeOpt as a simple four-step process that requires retail partners to "add our retargeting tag to your website so we can match your shoppers back to our database of 175+ people. As shoppers engage on your website and bounce off, we'll match their cookies against our database and send to people we can.[6]

AddShoppers explicitly markets its cross-site tracking capabilities: "When visitors come to our clients' websites, we can identify a large quantity of people that are known to our network, but unknown to the website."[7] It emphasizes "these are net-new people that they would have never been able to target without our network, because they didn't have that email in their database yet."[8] And the company encourages retailers to "market to people, not cookies."[9]

[5] Ex. 5, "Introducing Email Retargeting Co-op + SafeOpt Consumer Rights Management Integrated Platform."
[6] Ex. 6, at AS-00215.
[7] Ex. 7, "3 Reasons You Should Care About People-Based Marketing."
[8] *Id.*
[9] *Id.*

B. AddShoppers builds a massive network of shoppers using third party data brokers.

AddShoppers claims (depending on the source) to maintain a massive database of between [redacted] million shoppers.[10] [redacted]

But neither description really aligns with reality. The first channel is mostly nonexistent: almost nobody signs up directly for SafeOpt. [redacted]

And although AddShoppers portrays its second channel as partnerships with legitimate websites that collect email addresses and add users to its network, the channel operates quite differently in practice. [redacted]

[10] Ex. 8, Smith Decl. ¶ 37; Ex. 6, at AS-215; Ex. 7.
[11] Ex. 6, at AS-00216.
[12] *Id.*
[13] Ex. 1, West Dep. 92:1-16.
[14] Ex. 1, West Dep. 92:17-25.
[15] Ex. 3, King Dep. 68:17-69:1; *see also* Ex. 1, West Dep. 84:3-17.
[16] Ex. 1, West Dep. 110:4-6; West Dep. 115:19-116:7. [redacted]

[redacted]

AddShoppers also acquires email addresses through its retail partners who agree to participate in its "Data Co-Op."[19] These addresses are typically collected when customers register or begin the registration process on a partner website.[20] [redacted]

C. AddShoppers develops a uniform tracking code designed to transmit detailed browsing information in real time.

AddShoppers developed JavaScript tracking technology that monitors users across retail websites by collecting detailed browsing information. [redacted] Once installed, the tracking code operates uniformly across a retailer's website (unless blocked).[23]

The tracking system captures extensive data through the combination of cookies and tracking pixels. [redacted]

[17] Ex. 1, West Dep. 103:6-10.
[18] Ex. 3, King Dep. 113:4-13.
[19] Ex. 8, Smith Decl. ¶ 38; Ex. 3, King Dep. 62:16-64:11.
[20] Ex, 8, Smith Decl. ¶ 38.
[21] Ex. 3, King Dep. 62:16-64:11.
[22] Ex. 3, King Dep. 91:17-21; Ex. 9.
[23] Ex. 3, King Dep. 98:10-16; 169:19-21.
[24] Ex. 8, Smith Decl. ¶¶ 22, 42; Ex. 3, King Dep. 33:24-34:17.
[25] Ex. 3, King Dep. 34:7:17.

The system monitors the "conversation" between shoppers and websites in real time throughout each browsing session.[26] [redacted] As shoppers navigate the website, browse products, add items to carts, and complete purchases, the tracking code captures and transmits this information to AddShoppers.[28]

[redacted]

D. AddShoppers maintains an identity graph on shoppers.

AddShoppers maintains a vast database linking personal information (individual email addresses) with detailed browsing activity across thousands of retailers.[33] [redacted]

[26] Ex. 8, Smith Decl. ¶¶ 46-48.
[27] Clayton Dep. 88:2-89:21 (the Clayton deposition transcript is attached to the Youngentob Declaration as Ex. 10).
[28] Ex. 8, Smith Decl. ¶¶ 46-48.
[29] Ex. 8, Smith Decl. ¶ 56; Ex. 3, King Dep. 39:23-42:14.
[30] Ex. 8, Smith Decl. ¶ 56.
[31] *Id.*
[32] *Id.*
[33] Ex. 8, Smith Decl. ¶¶ 26, 33.
[34] Ex. 8, Smith Decl. ¶ 55.
[35] Ex. 6, at AS-221.

[redacted]

[redacted]

[redacted]

[36] Ex. 3, King Dep. 74:24-77:2.
[37] Ex. 10, Clayton Dep. 81:10-19.
[38] Ex. 11.
[39] Ex. 11; Ex. 6, at AS-00215; Ex. 1, West Dep. 121:1-10.

[redacted] The system operates by leveraging this shared pool of user data collected through AddShoppers' technology.[43]

E. AddShoppers does not prioritize individual consent.

AddShoppers has given low priority to ensuring users explicitly consent to being tracked within its network. [redacted]

[40] Ex. 3, King Dep. 157:1-8.
[41] Ex. 3, King Dep. 59: 12-20.
[42] Ex. 10, Clayton Dep. 90:18-22.
[43] Ex. 12.
[44] Ex. 1, West Dep. 101:4-13.
[45] Ex. 1, West Dep. 102:4-103:5.
[46] Ex. 2, Ledford Dep. 156:10-157:9.
[47] Ex. 6, at AS-00215; Ex. 1, West Dep. 156:10-157:9.

[redacted]

F. Peet's partners with AddShoppers to track and email anonymous shoppers.

[redacted]

[48] Ex. 1, West Dep. 164:12-165:11.
[49] Ex. 13.
[50] Georgianna Dep. 57:7-13 (the Georgianna deposition transcript is attached to the Youngentob Declaration as Ex. 14).
[51] Hahm Dep. 85:1-9 (the Hahm deposition transcript is attached to the Youngentob Declaration as Ex. 15).
[52] Ex. 15, Hahm Dep. 115:14-117:5.
[53] Ex. 15, Hahm Dep. 42:7-10.
[54] Ex. 13.
[55] Ex. 14, Georgianna Dep. 50:18-53:10.
[56] Ex. 15, Hahm Dep. 65:15-66:2.
[57] Ex. 10, Clayton Dep. 110:20-25.

Even before implementing the tracking code, Peet's anticipated privacy concerns. [redacted]

G. Peet's configured SafeOpt tracking code to capture the content of its website visitors' communications.

[redacted]

[58] Ex. 16, at PEETS-168; Ex. 14, Georgianna Dep. 57:15-58:12.
[59] Ex. 16, at PEETS-167.
[60] Ex. 14, Georgianna Dep. 26:1-8; 42:3-9; 44:8-11.
[61] Ex. 15, Hahm Dep. 30:12-18.
[62] Ex. 15, Hahm Dep. 60:17-61:8; Ex. 14, Georgianna Dep. 55:10-12; Ex. 3, King Dep. at 28:1-11, 47:14-22, 52:14-20.
[63] Ex. 2, Ledford Dep. 119:14-19.
[64] Ex. 14, Georgianna Dep. 79:2-80:6.
[65] Ex. 15, Hahm Dep. 83:18-22.
[66] Ex. 2, Ledford Dep. 108:10-21; Ex. 14, Georgianna Dep. 80:25-81:5.

H. [redacted]

[67] Ex. 17; Ex. 14, Georgianna Dep. 63:12-72:17.
[68] Ex. 17.
[69] Ex. 18, at PEETS-239.
[70] Ex. 18, at PEETS-238.
[71] Ex. 14, Georgianna Dep. 71:13-17.

I. Peet's continues transmitting detailed browsing information to AddShoppers after their partnership ends.

[redacted]

J. Peet's fails to properly disclose or control its data sharing.

For over three years, while AddShoppers' code secretly harvested user data from Peet's website, Peet's privacy policies concealed this practice. Between March 17, 2021, and August 28, 2024, Peet's cycled through five different privacy policies—not one disclosed the embedded code was automatically transmitting users' detailed browsing data to AddShoppers' database, where it was associated with their personal information.[75] [redacted]

Peet's made just one fleeting reference to AddShoppers during a 73-day window—from January 12, 2024, to March 25, 2024—after this litigation began. Even then, the disclosure was telling: while Peet's thoroughly detailed Google's tracking program, it offered only a cursory mention of AddShoppers, omitting any explanation of its tracking network or the Data Co-op.[76] A[redacted] Peet's then scrubbed all references to AddShoppers from its privacy policy on March 25, 2024[redacted]

[72] Ex. 15, Hahm Dep. 104:8-13.
[73] Ex. 8, Smith Decl. ¶ 61; Ex. 19.
[74] Ex. 3, King Dep. 183:18-186:18; Ex. 9 and Ex. 20.
[75] Peet's privacy policies (Exs. 21-25).
[76] Ex. 14, Georgianna Dep. 129:17-130:9.
[77] Ex. 10, Clayton Dep. 110:11-19.
[78] Ex. 19.

Peet's consent management system was also a façade. [redacted] Besides, Peet's began tracking visitors immediately upon landing on its website, regardless of whether they interacted with the cookie banner.[83] [redacted]

K. AddShoppers captures Plaintiffs' detailed browsing activities through its retail partners.

AddShoppers tracked each Plaintiff extensively across the internet for several years, collecting detailed records about their visits to various retailers' websites. The data AddShoppers collected included the exact products Plaintiffs viewed or added to their carts, along with prices.[85] For example, Abby Lineberry's data showed when she visited Dia & Co.'s website and the Navy Olivia Cross-Back Blouse she added to her cart.[86] Similarly, Mike Cook's data showed when he visited Peet's website and the exact coffee products he added to his cart.[87] AddShoppers data also

[79] Dkt. 51-1 at 2; Ex. 14, Georgianna Dep. 85:6-20.
[80] Ex. 14, Georgianna Dep. 89:9-12.
[81] Ex. 14, Georgianna Dep. 89:21-91:11.
[82] *Id.*
[83] Ex. 14, Georgianna Dep. 86:18-88:2.
[84] *Id.*
[85] Ex. 3, King Dep. 139:16-148:2 ([redacted]); *see also* Ex. 26.
[86] Ex. 27, Lineberry Decl.
[87] Ex. 28, Cook Decl.

shows Miguel Cordero's visit to Peet's, which means his visit met the behavioral criteria to transmit his browsing activity to AddShoppers.[88] And because Peet's campaign configurations required the collection of detailed browsing activity, AddShoppers must have been transmitted this type of information during his visit.[89]

III. Legal Standard

To certify a class, plaintiffs must show numerosity, commonality, typicality, and adequacy. Fed. R. Civ. P. 23(a). For money damages classes, plaintiffs must also demonstrate predominance and superiority. Fed. R. Civ. P. 23(b)(3). And for injunctive relief classes, plaintiffs must instead show that "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2).

IV. The Proposed Classes and Subclasses

Plaintiffs respectfully seek to certify the following classes, with Plaintiffs Cook and Cordero serving as class representatives for the nationwide CDAFA class against Peet's, and Plaintiffs Lineberry and Cordero serving as class representatives for the California subclasses and the California injunctive relief class:

Nationwide CDAFA Class (against Peet's):

> All natural persons who visited Peet's website and for whom AddShoppers collected their detailed browsing activity.

California CIPA Subclass (against Peet's):

> All natural persons who, while in California, visited Peet's website for whom AddShoppers collected their detailed browsing activity.

California CDAFA and CIPA Subclass (against AddShoppers):

> All natural persons who, while in California, visited Peet's or Dia's websites for whom AddShoppers collected their detailed browsing activity.

[88] Ex. 2, Ledford Dep. 144:11-18, 145:12-16.
[89] Ex. 29, Cordero Decl.

California Injunctive Relief Class (against AddShoppers):

> All natural persons who, while in California, visited a website for whom AddShoppers collected their detailed browsing activity.

The proposed classes and subclasses exclude persons who directly enrolled in the SafeOpt program operated by AddShoppers; any officers and directors of Defendants; class counsel; and the judicial officers presiding over this action and the members of their immediate family and judicial staff.

V. Legal Argument

A. The classes satisfy the Rule 23(a) factors.

1. The classes are numerous.

The classes are "so numerous that joinder of all members is impracticable." Rule 23(a)(1). Numerosity is generally satisfied when a proposed class contains at least 40 members. *Akaosugi v. Benihana Nat'l Corp.*, 282 F.R.D. 241, 253 (N.D. Cal. 2012). And AddShoppers collected detailed browsing information on [redacted] across Peet's and Dia's websites.[90]

2. The classes present common issues of fact and law.

The classes present common "questions of law or fact." Fed. R. Civ. P. 23(a)(2). The commonality requirement is not an onerous one: even "a single common question" will do. *Franklin v. Midwest Recovery Sys., LLC*, 2021 WL 1035121, at *2 (C.D. Cal. Feb. 5, 2021) (citation omitted). Here, common questions include:

- Whether AddShoppers acted willfully
- Whether the detailed product browsing information that AddShoppers captured was "content" covered by CIPA
- Whether the information was intercepted in real time
- Whether Peet's aided AddShoppers' violations
- Classwide damages.

These common questions of law and fact easily satisfy the commonality requirement.

[90] Ex 30.

3. Plaintiffs' claims are typical.

Plaintiffs satisfy typicality because their claims all "arise from the same course of events, and each class member makes similar legal arguments to prove the defendant's liability." *Cal. Coal. for Women Prisoners v. United States*, 723 F. Supp. 3d 712, 730 (N.D. Cal. 2024) (citation omitted); *see also Scholl v. Mnuchin*, 489 F. Supp. 3d 1008, 1044 (N.D. Cal. 2020) (similar). Like all class members, Plaintiffs had their detailed browsing activity captured by SafeOpt tracking code.[91] Because all the claims arise from Defendants' use of the tracking code to intercept this information, typicality is satisfied.

4. Plaintiffs and their counsel will adequately represent the classes.

Plaintiffs and their counsel will "fairly and adequately protect the interests of the class," Fed. R. Civ. P. 23(a)(4), because (1) they do not have any conflicts of interest with other class members and (2) have vigorously advanced the interests of the class throughout this litigation. *See Staton v. Boeing Co.*, 327 F.3d 938, 957 (9th Cir. 2003) (outlining adequacy standard).

Plaintiffs have no conflicts of interest with other class members. Plaintiffs have also shown that they are adequate class representatives who are willing to vigorously prosecute this action through trial. Plaintiffs already made significant contributions to the litigation, including by assisting in preparing the complaints, gathering records, responding to written discovery requests, appearing for depositions, consulting counsel on case developments and strategy, and submitting declarations in support of this motion.[92] *See Castro v. ABM Indus., Inc.*, 325 F.R.D. 332, 342 (N.D. Cal. 2018) (plaintiffs were adequate where they "ha[d] been active participants in the litigation").

Plaintiffs' counsel have also demonstrated their adequacy under Rule 23(g), which focuses on "(1) the work counsel has done in identifying or investigating potential claims in the action; (2) counsel's experience in handling class actions or other complex litigation and the type of claims in the litigation; (3) counsel's knowledge of the applicable law; and (4) the resources that counsel

[91] *See* Supra § II.K.
[92] Exs. 27, 28, 29 (Plaintiff Decl.)

will commit to representing the class." *Scholl*, 489 F. Supp. 3d at 1045. The attorneys from Stueve Siegel Hanson LLP and Gibbs Law Group are experienced in prosecuting privacy and consumer class actions.[93] They have dedicated substantial time and resources to investigating, pleading, and pursuing these claims, and demonstrated their knowledge of the applicable law, including in opposition to Defendants' motions to dismiss.[94] Accordingly, Plaintiffs request that the Court appoint attorneys from Stueve Siegel Hanson and Gibbs Law Group to serve as class counsel under Rule 23(g).

B. The classes satisfy the Rule 23(b)(3) factors.

1. Common questions predominate over individual questions.

The "classes are sufficiently cohesive to warrant adjudication by representation." *Amchem Prod., Inc. v. Windsor*, 521 U.S. 591, 623 (1997). When evaluating predominance, courts examine the "relation between common and individual questions in a case." *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016). While individual questions require "evidence that varies from member to member," common questions rely on the same evidence across all members. *Id.* Not all questions must be common for a class to meet this requirement. Rather, the predominance analysis essentially asks whether common questions outweigh individual issues in importance. *See id.*

The Court should begin its predominance analysis "with the elements of the underlying cause of action." *Erica P. John Fund, Inc. v. Halliburton Co.*, 563 U.S. 804, 809 (2011). Here, if class members pursued their claims individually, each case would require identical evidence about Defendants' conduct to support their claims.

[93] Ex. 31 (Firm Resumes).
[94] Youngentob Decl. ¶

a. Common issues predominate for the CIPA claim.

i. Common evidence proves Defendants' liability for violating CIPA.

Under CIPA, Plaintiffs must show AddShoppers "(1) willfully (2) and without Plaintiffs' consent (3) read or attempted to read or learn the contents of their communications (4) while the communications were being sent from, received in, or in transit or passing over any wire, line or cable in California." *Torres v. Prudential Fin., Inc.*, 2024 WL 4894289, at *4 (N.D. Cal. Nov. 26, 2024). Peet's, in turn, is liable for aiding and abetting AddShoppers' violation. *Id.*

Predominance is satisfied because both liability theories focus on Defendants' uniform conduct toward all class members, which can be proven through common evidence. *See Flowers v. Twilio, Inc.*, 2018 WL 10758024, at *5 (Cal. Super. Ct. Jan. 02, 2018) (predominance met for CIPA class, noting that defendant "acted uniformly as to each class member") (citation omitted); *Zaklit v. Nationstar Mortg. LLC*, 2017 WL 3174901, at *10 (C.D. Cal. July 24, 2017) (predominance met for CIPA class); *Raffin v. Medicredit, Inc.*, 2017 WL 131745, at *9 (C.D. Cal. Jan. 3, 2017) (same).

AddShoppers acted willfully. AddShoppers' willfulness can be proven through its intentional design and deployment of the SafeOpt tracking technology.[95] AddShoppers has [redacted]. *See Romero v. Securus Techs., Inc.*, 331 F.R.D. 391, 411 (S.D. Cal. 2018) (holding that defendant's knowledge under CIPA was a predominant issue suitable for classwide proof).

AddShoppers captured the content of the class members' communications. Plaintiffs can prove through common evidence that AddShoppers captured the content of class members' communications. Courts have consistently held that detailed browsing information revealing users' interests and interactions qualifies as protected content. *See Mata v. Zillow Grp., Inc.*, 2024

[95] *See* Supra § II.C.

WL 5161955, at *5 (S.D. Cal. Dec. 18, 2024) (holding that information revealing "personal interests, queries, and habits" constitutes protected content) (quoting *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 605 (9th Cir. 2020)); *Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041, at *5 (N.D. Cal. Dec. 30, 2024) (holding that intercepted information showing "content categories and details" constitutes protected content).

AddShoppers tracking technology is specifically designed to capture detailed browsing information, including product names, prices, SKUs, and product images.[96] [redacted] The captured data goes well beyond basic identification information to reveal users' substantive interests and interactions with specific products. *See Yoon*, 2024 WL 5264041, at *5 (finding content where data "shed[s] light on people's interests" and is "descriptive of the content").

AddShoppers intercepted class members' communications in real time. Plaintiffs can prove through common evidence that AddShoppers captured communications in real time.[98] AddShoppers' own documents reveal that the tracking pixel transmits information contemporaneously with website interactions. [redacted] *See Yockey v. Salesforce, Inc.*,

[96] *See* Supra § II.C.
[97] Ex. 3, King Dep. 28:1-11 ([redacted] (emphasis added)); Ex. 15, Hahm Dep. 60:22-24 ([redacted]).
[98] *See* Supra § II.C.
[99] Ex. 8, Smith Decl. ¶¶ 46-48.

2024 WL 3875785, at *5 (N.D. Cal. Aug. 16, 2024) (distinguishing cases where data was accessed from storage or "after receipt by the intended recipient" from real-time interception claims)

AddShoppers intercepted class members' communications in California. Plaintiffs can establish through common evidence that AddShoppers captured communications where class members were physically located. As Plaintiffs' expert states, "JavaScript code for the SafeOpt tag is executed in a consumer's browsers."[100] Thus, "the transmission happens where a consumer is physically located."[101] Plaintiffs can then reliably identify class members through multiple verification methods: (1) AddShoppers' database provides a comprehensive list of potential class members whose communications were captured; (2) class members can self-identify as California residents; (3) [redacted] This combination of self-identification and objective verification through IP addresses provides a reliable mechanism for identifying class members whose communications were intercepted while they were in California.

Class members did not consent to Defendants' practices. Plaintiffs can prove the lack of consent through common evidence. CIPA requires "prior consent of all parties to a communication," *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022), and such consent must be knowingly given. *Negro v. Superior Ct.*, 230 Cal. App. 4th 879, 892 (2014). Neither requirement was met here:

First, AddShoppers made no direct attempts to secure consent from users.[102] It instead delegated this responsibility entirely to website owners and took no steps to ensure they obtained adequate consent. *See Romero*, 331 F.R.D. at 411 (finding consent was a common question where defendant uniformly failed to obtain it).

[100] Ex. 8, Smith Decl. ¶ 35.
[101] *Id.*
[102] *See* Supra § II.E.

Second, neither Peet's nor Dia's privacy policies ever provided legally sufficient notice during the class period.[103] This uniform failure to disclose is fatal because actual consent, whether express or implied, requires explicit notification of the specific practice at issue. *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022). A "generalized notice is not sufficient to establish consent." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793 (N.D. Cal. 2022); *see also Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) (requiring notice of "specific practice[s]").

Peet's is liable for aiding and abetting on a classwide basis. Plaintiffs can prove Peet's liability for aiding and abetting AddShoppers' CIPA violations through common evidence. Under California law, aiding and abetting liability attaches when a defendant "knows the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other to so act." *In re Woodbridge Invs. Litig.*, 2020 WL 4529739, at *5 (C.D. Cal. Aug. 5, 2020). Common evidence proves both elements.

First, [redacted]

Second, Peet's provided substantial assistance. SafeOpt's operation requires two essential participants: AddShoppers as the script provider and the website owner as the script installer. [redacted]

Because Peet's actions were uniform across all class members, its aiding and abetting liability can be determined on a classwide basis. *See Takiguchi v. MRI Int'l, Inc.*, 2016 WL

[103] *See* Supra § II.J.; *see also* Ex. 32 (Dia Privacy Policy)
[104] *See* Supra § II.F-G.
[105] *Id.*

1091090, at *10-11 (D. Nev. Mar. 21, 2016) (finding predominance met for aiding and abetting claims based on common evidence).

ii. Plaintiffs can calculate classwide statutory damages under CIPA.

For their CIPA claim, Plaintiffs only intend to seek statutory damages of $5,000 per violation. Cal. Penal Code § 637.2(a). Courts consistently hold that such statutory damages can be calculated on a classwide basis through a straightforward formula: multiplying the number of proven violations by the statutory amount. *See Kellman v. Spokeo, Inc.*, 2024 WL 2788418, at *11 (N.D. Cal. May 29, 2024) (finding statutory damages calculations under CIPA present common questions that predominate for class certification purposes); *Coulter v. Bank of Am.*, 28 Cal. App. 4th 923, 925 (1994) (affirming $132,000 award calculated as $3,000 for each of 44 CIPA violations). And here, AddShoppers' records provide a definitive list of potential class members and the date of each violation.[106] As a result, determining classwide damages is a matter of multiplication. *See Doe v. Mindgeek USA Inc.*, 702 F. Supp. 3d 937, 950-51 (C.D. Cal. 2023).

b. Common issues predominate for the CDAFA claim.

i. CDAFA applies nationwide to Peet's conduct.

California law presumptively applies because Peet's maintains its global headquarters and key leadership in California. *See Ward v. United Airlines, Inc.*, 9 Cal. 5th 732, 750 (2020) (holding California statutes apply to conduct within California's borders absent evidence of intended limitation). Peet's also made the relevant decisions to partner with AddShoppers and to add the tracking technology in California. Courts routinely apply California law to nationwide classes in similar circumstances. *See, e.g.*, *Rodriguez v. Google, LLC*, 2024 WL 38302, at *13 (N.D. Cal. Jan. 3, 2024) (certifying nationwide classes for California privacy claims); *Doe v. Meta Platforms, Inc.*, 690 F.Supp.3d 1064, 1079 (N.D. Cal. 2023) (applying CIPA nationwide where technology design and implementation occurred in California); *Parkinson v. Hyundai Motor Am.*, 258 F.R.D.

[106] *See* Supra § II.D.

580, 599 (C.D. Cal. 2008). Because Plaintiff have shown California has "significant contact or significant aggregation of contacts" to class claims, the burden shifts to defendants to demonstrate why foreign law should apply instead. *Kearney v. Hyundai Motor Am.*, 2012 WL 13049699, at *7 (C.D. Cal. Dec. 17, 2012). The "application of California law here poses no constitutional concerns." *In re Qualcomm Antitrust Litig.*, 292 F. Supp. 3d 948, 978 (N.D. Cal. 2017).

ii. Common evidence proves Defendants' liability for CDAFA.

CDAFA provides a private right of action when defendants either: (1) "knowingly accesses and without permission takes, copies, or makes use of any data from a computer," Cal. Penal Code § 502(c)(2); or (2) "knowingly and without permission provides or assists in providing a means" of "accessing a computer, computer system, or computer network in violation of this section," Cal. Penal Code § 502(c)(6). *See Ticketmaster LLC v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1176 (C.D. Cal. 2018) (finding violation of subsection (c)(6) where defendant provided means for others to violate CDAFA). The statute also covers unauthorized use or access of computer services and systems. Cal. Pen. Code §§ 502(c)(3), (7).

Here, common evidence shows class members did not consent to Defendants' data collection. *See Greenley v. Kochava, Inc.*, 2023 WL 4833466, at *13 (S.D. Cal. July 27, 2023) (holding the "without permission" element is satisfied where a plaintiff "did not 'consent' to Defendant's data collection.").

iii. Common evidence proves class members' damages under CDAFA.

The CDAFA protects "the privacy of individuals" through safeguards for "lawfully created computers, computer systems, and computer data." Cal. Pen. Code § 502(a). Plaintiffs have recently discovered AddShoppers purchases personal information on a per-record basis, demonstrating that the misappropriated data carries quantifiable financial value. *See Frasco v. Flo Health, Inc.*, 2024 WL 4280933, at *3 (N.D. Cal. Sept. 23, 2024) (finding evidence that misappropriated information "carried financial value" sufficient to establish damage or loss under

CDAFA); *Rodriguez*, 2024 WL 38302, at *6 (certifying CDAFA class based on classwide evidence of data's financial value and defendants' profits).

The misappropriation of valuable data constitutes sufficient harm to support CDAFA claims, and the statute does not require precise individual loss calculations. *See NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 964 (N.D. Cal. 2014) ("[A]ny amount of damage or loss caused by the defendant's CDAFA violation is enough to sustain the plaintiff's claims.").

2. Class treatment is superior to individual litigation.

Class treatment is "superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). Courts evaluate superiority by considering: (1) class members' interest in individually controlling separate actions; (2) the extent and nature of existing litigation by class members; (3) the desirability of concentrating claims in the particular forum; and (4) likely management difficulties. *Id.*

Each factor strongly favors class treatment here. First, class members lack a compelling interest in individual prosecution because the cost of litigating individual cases would substantially exceed potential damages. Second, no other cases alleging CIPA violations are pending against Defendants. Third, consolidation in this forum ensures class members can vindicate their rights.

3. This case is manageable as a class action.

This case is readily manageable as a class action. The claims at issue do not present individualized questions that would overwhelm the trial. Both claims focus on whether Defendants unlawfully intercepted and used consumers' data without consent, a question that will be resolved through common evidence applicable to the entire class.[107] For example, whether AddShoppers' tracking technologies violated CIPA by intercepting communications without consent is an identical question for all class members, as the tracking technology operates in the same way for all website visitors. Similarly, whether AddShoppers accessed consumers' data on a computer or network without permission in violation of CDAFA is a uniform question that applies equally to

[107] Ex 33 (Proposed Verdict Form)

all class members. There is no need for individualized inquiries into each consumer's experience; the focus remains on Defendants' standardized conduct.

To further ensure the case remains efficient and manageable, Plaintiffs tailored their class definitions to focus narrowly on specific retailers whose privacy policies clearly fail to disclose AddShoppers' tracking practices. By doing so, Plaintiffs have minimized any risk that individualized issues, such as lack of consent, will predominate over the common ones.

Additionally, AddShoppers' own database provides a straightforward and reliable method for identifying class members. The database contains detailed records of website visits tied to specific email addresses, along with geolocation data such as IP addresses. As a result, notice can be issued directly via email, using AddShoppers' own comprehensive database, and self-identification can be further verified through the geolocation data it collected. Courts regularly approve far less robust methods for identifying class members in data privacy cases. *See, e.g.*, *Kellman*, 2024 WL 2788418, at *11, *15 (approving self-identification and claims administration process using common evidence to determine class membership).

This case also presents no choice of law complications that would hinder class certification. The claims are based solely on two California statutes. And the relevant conduct—AddShoppers' data collection and tracking practices—directly targeted California residents through websites accessible in the state. Thus, California law applies uniformly to the proposed class, avoiding any complex multi-state legal analysis.

C. Rule 23(b)(2) certification is also warranted.

Plaintiffs seek certification under Rule 23(b)(2) for injunctive relief.[108] *See Brown v. Google, LLC*, 2022 WL 17961497, at *19-20 (N.D. Cal. Dec. 12, 2022) (certifying injunctive CDAFA and CIPA class); *In re Google RTB Consumer Priv. Litig.*, 2024 WL 2242690, *15 (N.D. Cal. Apr. 4, 2024) (finding "plaintiffs' motion for an injunctive relief class under Rule 23(b)(2)

[108] The Court may certify claims under both Rule 23(b)(3) and 23(b)(2). *See In re Xyrem (Sodium Oxybate) Antitrust Litig.*, 2023 WL 3440399, at *12 (N.D. Cal. May 12, 2023).

would be appropriate for purposes of plaintiffs' claims under the UCL and CIPA"). Rule 23(b)(2) certification is appropriate when plaintiffs challenge centralized policies that do not require individualized injunctive relief. *See B.K. ex rel. Tinsley v. Snyder*, 922 F.3d 957, 971 (9th Cir. 2019). Courts do not examine the viability of class members' claims for declaratory and injunctive relief; they consider only "whether class members seek uniform relief from a practice applicable to all of them." *Ward v. United Airlines, Inc.*, 2021 WL 534364, at *7 (N.D. Cal. Feb. 12, 2021) (citation omitted).

Plaintiffs seek injunctive relief to (1) prohibit AddShoppers from collecting class members' detailed browsing data through the tracking pixel; (2) require AddShoppers to delete all class members' data; and (3) appoint an independent third party to verify that the injunctive relief has been implemented. This requested relief is sufficiently detailed at this juncture and is practical to implement, particularly given that AddShoppers already employs geolocation data from IP addresses to block tracking of individuals from certain geographic locations. Rule 23(b)(2) "ordinarily will be satisfied when plaintiffs have described the general contours of an injunction that would provide relief to the whole class, that is more specific than a bare injunction to follow the law, and that can be given greater substance and specificity at an appropriate stage in the litigation." *Parsons v. Ryan*, 754 F.3d 657, 689 n.35 (9th Cir. 2014).

"Unlike Rule 23(b)(3), a plaintiff does not need to show predominance of common issues or superiority of class adjudication to certify a Rule 23(b)(2) class." *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 587 (N.D. Cal. 2015); *see also id.* (certifying injunctive relief class requesting Yahoo to stop scanning emails and explaining that Yahoo's "focus on whether a potential class member has consented to Yahoo's [conduct] loses sight of the purpose of Rule 23(b)(2)"). Plaintiffs need only "sufficiently identif[y] the specific course of conduct that plaintiffs seek to enjoin" and "establish[] that this course of conduct applies to the entire proposed class." *Brown*, 2022 WL 17961497, at *20.

VI. Mr. Clayton's testimony should be excluded under Federal Rule of Evidence 702.

The testimony of AddShoppers' expert, Will Clayton, should be excluded under Rule 702. "An expert's testimony must be both relevant and reliable." *Dep't of Toxic Substances Control v. Technichem, Inc.*, 2016 WL 1029463, at *1 (N.D. Cal. Mar. 15, 2016) (cleaned up). Mr. Clayton's opinions fail on both counts. *See id.* (excluding expert who "often d[id] no more than regurgitate information given to him by other sources (including self-serving assertions by the defendants)").

A. Mr. Clayton's opinion that AddShoppers' software is "common" is unreliable.

Mr. Clayton's opinion that AddShoppers' software is "more than common" hinges on two fatally flawed assumptions.[109]

First, [redacted] His conclusion therefore lacks a factual basis and is refuted by the very evidence he failed to consider.

[109] Ex. 34, Clayton Decl. ¶ 9; Ex. 10, Clayton Dep. 11:10-19
[110] Ex. 10, Clayton Dep. 68:18-69:13.
[111] Ex. 6, at AS-00216
[112] *Id.*
[113] *See* Ex. 10, Clayton Dep. 67:16-68:15.

Second, [redacted] This definition is not supported by Defendants' own privacy policies, nor is it consistent with relevant privacy laws, including the CCPA, which explicitly recognizes email addresses as personal information precisely because they can be linked to a particular individual.[116] [redacted]

Without these assumptions, [redacted] Besides, the mere prevalence of a technology does not determine its legality or compliance with privacy laws.

[114] Ex. 10, Clayton Dep. 69:15-70:13

[115] *Id.*

[116] Ex. 10, Clayton Dep. 121:13-122:24. *See* Cal. Civ. Code § 1798.140(v)(1) (defining "Personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" including "[i]dentifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, *email address*, account name, social security number, driver's license number, passport number, or other similar identifiers.") (emphasis added).

[117] Ex. 10, Clayton Dep. 57:19-60:17

[118] Ex. 10, Clayton Dep. 56:13-20, 102:4-20.

B. Mr. Clayton's privacy policy opinions are neither reliable nor relevant.

Mr. Clayton's opinions about Peet's privacy policy disclosures directly contradict the law for two reasons.

First, [redacted] But in this context, consent requires explicit notification of the specific practice at issue. *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d at 949. [redacted]

Second, [redacted] *See Calhoun v. Google, LLC*, 113 F.4th 1141, 1151 (9th Cir. 2024). Just the opposite. [redacted] . *See Calhoun*, 113 F.4th at 1151 (explaining consent is evaluated by the sophistication level attributable to the general public). [redacted]

[119] Ex. 10, Clayton Dep. 123:5-13.
[120] Ex. 10, Clayton Dep. 117:1-24.
[121] *Id.*
[122] Ex. 34, Clayton Decl. ¶ 52.
[123] Ex. 10, Clayton Dep. 113:14-22.

[redacted] Consequently, Mr. Clayton's opinion is not just irrelevant; it distorts the facts and risks confusing the issue of consent altogether.

VII. Conclusion

For the reasons set forth herein, Plaintiffs respectfully request that the Court grant their motion for class certification and to exclude the testimony of Will Clayton.

Dated: January 7, 2025

Respectfully submitted,

/s/ *Kasey A. Youngentob*
Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
Kasey Youngentob (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100 (tel.)
siegel@stuevesiegel.com
moore@stuevesiegel.com
youngentob@stuevesiegel.com

David M. Berger (SBN 277526)
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9713
Facsimile: (510) 350-9701
dmb@classlawgroup.com